

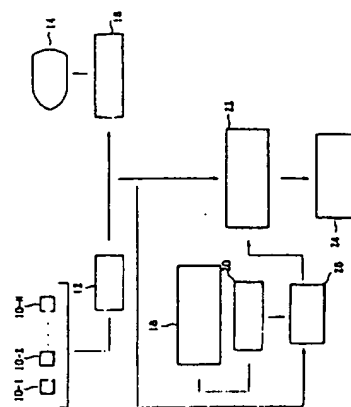
☆ (54) VISUAL IC CARD

(11) 4-255089 (A) (43) 10.9.1992 (19) JP  
 (21) Appl. No. 3-36674 (22) 6.2.1991  
 (71) FUJITSU LTD (72) HIROSHI TANAKA  
 (51) Int. Cl.<sup>5</sup> G06K19/10, B42D15/10, G06K19/07

**PURPOSE:** To provide an extremely effective visual IC card having many functions and excellent security with respect to an ID card to be used for a cash card, a credit card, a medical card, etc., especially provided with an input key and a display device.

5 **CONSTITUTION:** A data input means 12 inputs data corresponding to the operation of keys 10-1 to 10-N and an input data display means 16 displays the inputted data on a display device 14. Plural applications are previously written in an application storing means 18 and an identification(ID) data storing means 20 previously stores application ID data. A data collating means 22 collates the inputted data with the application ID data and a person-confirming means 24 confirms a card user as the owner when a positive collated result is obtained.

the the



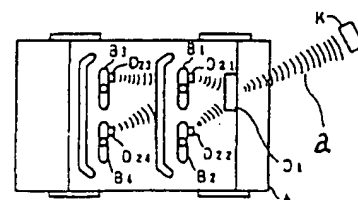
26: ID data reading means

(54) IDENTIFICATION SYSTEM FOR VEHICLE IN/OUT MANAGEMENT

(11) 4-255090 (A) (43) 10.9.1992 (19) JP  
 (21) Appl. No. 3-9585 (22) 30.1.1991  
 (71) MEIDENSHA CORP (72) KAZUYUKI KUMAKI  
 (51) Int. Cl.<sup>5</sup> G07C9/00, B42D15/10, G06F15/21, G06K17/00, G08G1/017

**PURPOSE:** To automatically execute vehicle identification(ID) and the personal ID of a person getting on a vehicle and to simplify management by making a vehicle ID device loaded on a vehicle to inquire a personal ID card carried by a person getting on the vehicle at the time of passing a gate and transmit a personal ID code together with a vehicle ID code to a vehicle detector.

**CONSTITUTION:** When a vehicle A passes a gate, the vehicle detector K sends an access signal to a vehicle ID device D<sub>1</sub>. The device D<sub>1</sub> transmits an inquiry signal from a transmission part to the inside of the vehicle at the period of about one minute. Persons B<sub>1</sub> to B<sub>n</sub> getting on the vehicle respectively carry respective personal ID cards D<sub>21</sub> or the like. After receiving the inquiry signal, respective cards D<sub>21</sub> or the like transmit personal ID codes. Each personal ID card is provided with an inherent queue time based on a registered number to prevent the generation of signal collision. The device D<sub>1</sub> transmits the vehicle ID code and the personal ID codes to the detector K. The detector K manages the IN/OUT of the vehicle and the persons getting on the vehicle in accordance with these codes.



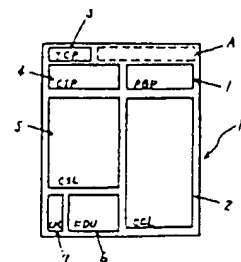
a: signal wave

(54) CASH DISPENSER

(11) 4-255091 (A) (43) 10.9.1992 (19) JP  
 (21) Appl. No. 3-36901 (22) 6.2.1991  
 (71) NEC CORP (72) YOSHIMI KITAGAWA  
 (51) Int. Cl.<sup>5</sup> G07D1/00, G07D9/00

**PURPOSE:** To improve the operation convenience of a cash dispenser by providing the cash dispenser body with a consumption medium stock rack for storing consumption medium so as to always store the consumption medium.

**CONSTITUTION:** The cash dispenser body M is provided with a bankbook printer unit 1, a paper money processing unit 2, a card processing unit 4, or the like. The consumption medium stock rack A is arranged on a space position in the upper area of the dispenser body M. The stock rack A is formed by reinforced glass or reinforced plastic so that the inside can be observed and the number of remaining medium can be checked at a glance from the external. The stock rack A is laterally arranged and provided with a bankbook storing rack, a certificate storing rack, a receipt form storing rack, a journal form storing rack, a depositing/paying form storing rack, and a transfer card storing rack. Respective racks are provided with locking keys so as to store important medium.



特開平4-255089

(43) 公開日 平成4年(1992)9月10日

(51) Int.Cl. <sup>3</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 19/10				
B 4 2 D 15/10	5 2 1	9111-2C		
G 0 6 K 19/07				
		8623-5L	G 0 6 K 19/ 00	R
		8623-5L		J
審査請求 未請求 請求項の数3 (全 6 頁)				

(21) 出願番号 特願平3-36674

(22) 出願日 平成3年(1991)2月6日

Application Date Feb. 6, 1991

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72) 発明者 田中 弘

神奈川県川崎市中原区上小田中1015 富士

通株式会社内

(74) 代理人 弁理士 伊藤 儀一郎

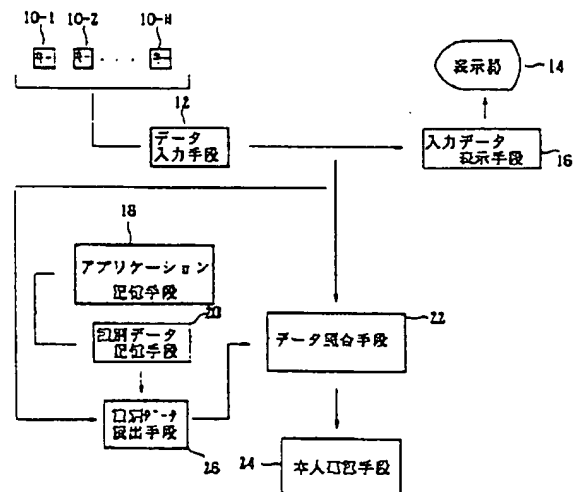
(54) 【発明の名称】 ビジュアル I C カード

(57) 【要約】

【目的】 本発明は、キャッシュカード、クレジットカード、医療カードなどに利用される I C カードにかかり、特に、入力キーと表示器が設けられた I C カードに関し、多機能でセキュリティに優れた極めて有用なビジュアル I C カードの提供を目的とする。

【構成】 キー 10-1、10-2・・・10-N の操作に応じたデータをデータ入力手段 12 が入力し、入力データ表示手段 16 は入力されたデータを表示器 14 に表示させる。アプリケーション記憶手段 18 には複数のアプリケーションが予め書き込まれ、識別データ記憶手段 20 はアプリケーション識別用のデータを予め記憶する。データ照合手段 22 は入力されたデータをアプリケーションの識別データと照合し、本人確認手段 24 は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

発明の概要説明図



1

## 【特許請求の範囲】

【請求項 1】 キー（10-1、10-2・・・10-N）の操作に応じたデータを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたデータをアプリケーションの識別データと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアル IC カード。

【請求項 2】 キー（10-1、10-2・・・10-N）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（26）と、入力されたアプリケーション固有データを読み出されたアプリケーション識別用のデータと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアル IC カード。

【請求項 3】 キー（10-1、10-2・・・10-N）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（26）と、入力されたアプリケーション固有データを読み出されたアプリケーションの識別データと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアル IC カード。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、キャッシュカード、クレジットカード、医療カードなどとして利用される IC カードにかかり、特に、入力キーと表示器が設けられた IC カードに関する。

2

【0002】 この種の IC カードには入力キーと表示器が設けられており、したがって、それらを用いてカード利用者の本人確認をカード単体で行なうことが可能となる。

## 【0003】

【従来の技術】 図 11 には IC カードシステムが示されており、キーボード 80 が処理装置 82（パーソナルコンピュータなど）に設けられている。

【0004】 この処理装置 82 にはカードリーダー・ライター 84 が接続されており、IC カード 86 はカードリーダー・ライター 84 にセットされる。

【0005】 そして、キーボード 80 の操作で処理装置 82 に PIN データが入力されると、この入力データが IC カード 86 へ送信される。

【0006】 その結果、カード利用者の本人確認が行なわれると、IC カード 86 を利用した取引が行なわれる。

【0007】 ところがこのシステムにおいては、本人確認用の PIN データが処理装置 82 へ入力されるので、PIN データの漏洩を確実に防止することが困難となる。

【0008】 そこで、図 2 のように複数のキー 10 と表示器 14 とを備え、これらキー 10、表示器 14 によってカード利用者の本人確認をカード単体で行なえるビジュアル IC カード 28 が利用される。

【0009】 従来においては、ビジュアル IC カード 28 に単一のアプリケーションが用意されており、したがって、その用途はキャッシュカード、クレジットカード、医療カードなどのいずれかに限られていた。

## 【0010】

【発明が解決しようとする課題】 MS カード（磁気カード）にはキャッシュカード、クレジットカードの機能が既に付与されているので、これより能力がはるかに高いビジュアル IC カード（28）にはより豊富な機能が要望される。

【0011】 本発明は上記従来の事情に鑑みてなされたものであり、その目的は、PIN データの漏洩を確実に防止できる多機能なビジュアル IC カードを提供することにある。

## 【0012】

【課題を解決するための手段】 上記目的を達成するために、本発明にかかるビジュアル IC カード（28）は図 1 のように構成されている。

【0013】 第 1 発明においては、キー 10-1、10-2・・・10-N の操作に応じたデータをデータ入力手段 12 が入力し、入力データ表示手段 16 は入力されたデータを表示器 14 に表示させる。

【0014】 また、アプリケーション記憶手段 18 には複数のアプリケーションが予め書き込まれ、識別データ記憶手段 20 はアプリケーション識別用のデータを予め

記憶する。

【0015】そして、データ照合手段22は入力されたデータをアプリケーションの識別データと照合し、本人確認手段24は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【0016】第2の発明においては、キー10-1、10-2・・・10-Nの操作に応じアプリケーション特定データとアプリケーション固有データをデータ入力手段12が入力し、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを識別データ読出手段26が読み出す。

【0017】データ照合手段22は入力されたアプリケーション固有データを読み出された各アプリケーションの識別データと照合し、本人確認手段24は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【0018】第3に発明においては、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を本人確認手段24が行なう。

【0019】

【作用】第1発明では、キー操作入力のデータをアプリケーションの識別データと照合した結果が肯定的なときに、カード利用者の本人確認が行なわれるので、カード利用者が本人であることと目的の機能（アプリケーション）を確認することが可能となる。

【0020】第2の発明では、目的の機能がカード利用者により特定されてから、そのアプリケーションに関する識別データとキー操作入力のデータが照合される。

【0021】第3の発明では、第2発明において肯定的な照合結果が得られた機能についてのみ、カード利用者の本人確認が行なわれる（図3参照）。

【0022】

【実施例】以下、図面に基づいて本発明にかかるビジュアルICカードの好適な実施例を説明する。

【0023】図2において、ビジュアルICカード28には複数のキー10と表示器14が設けられており、これらを用いてカード利用者の本人確認がカード単体で行なわれる。

【0024】このビジュアルICカード28はその本人確認が行なわれてから図4のカードリーダー・ライター84にセットされ、したがって、PINデータをキーボード80から処理装置82へ入力することを省略してその漏洩を防止できる。

【0025】本実施例のビジュアルICカード28には図5のように複数のアプリケーションデータファイル（ADF）1、2・・・が格納されており、このカード28がキャッシュカード及びクレジットカードとして利用される場合には、図6のようにそれらのアプリケーションデータファイル（1、2）が格納される。

【0026】そして、カード管理情報にはアプリケーシ

ョンデータファイル1、2・・・の個数が含まれており、これらアプリケーションデータファイル1、2・・・には相異なるPINデータ（通常は4桁）が各々含まれる（図6では"1234"、"5678"）。

【0027】また、ビジュアルICカード28には図7のキー制御部70、本人確認部72、コマンド部74が設けられており、キー操作で得られたデータはキー制御部10から本人確認部72へ入力される。

【0028】さらに、カード管理情報やアプリケーションデータファイル1、2・・・はコマンド部74によりアクセスされ、このコマンド部74で表示部14が制御される。

【0029】図8、図9には本人確認部72で行なわれる処理の内容がフローチャートで示されており、キー入力確認されると、処理ステータスのフラグがオンされているか否かが判断される（ステップ800）。

【0030】このフラグは電源の投入時にオフされており（電源の投入は図2の電源キーを操作することで行なわれる）、そのフラグ状態が確認されたときには、図10のように5桁長とされたPINバッファ90がクリアされる（ステップ802）。

【0031】さらに、アプリケーションデータファイル1、2・・・の数が読み出され（ステップ804）、その数が"1"かこれを越えているかが判定される（ステップ806）。

【0032】そして、アプリケーションデータファイルの数が"1"である場合（単機能カードの場合）には、入力データがPINバッファ90に格納されてその現行桁がインクリメントされ（ステップ808）、上記のフラグがオンされる（ステップ810）。

【0033】また、アプリケーションデータファイルの数が"1"を越えている場合（多機能カードの場合）には、キー入力データ（1桁）で示されるファイル名（そのファイルのPINデータ）が読み出され、セットされる（ステップ812）。

【0034】この後においては、4桁のキーデータがPINデータとして入力されるまで（ステップ814）、入力データをPINバッファ90に格納してその現行桁をインクリメントする処理（ステップ816）が繰り返される。

【0035】そして4桁のキーデータが（PINデータとして）入力されると（ステップ814）、処理ステータスのフラグがオフされる（ステップ818）。

【0036】次に、セット済みのファイル名（そのファイルに含まれたPINデータ）とキー操作入力のPINデータ（先頭4桁、最初に入力された後尾1桁はサフィックスとなる）とが突き合わされ（ステップ820・・・アプリケーションデータのファイル数が"1"である場合には、そのファイル名となるPINデータ）、両データの一致が確認されると（ステップ82

6

【図４】実施例のカードを取り扱うシステムの構成説明図である。

【図8】実施例の作用を説明するフローチャート（その1）である。

【図10】実施例で用意されるPINバッファの構成説明図である。

【符号の説明】

## 28 ビジュアルICカード

## 74 コマンド部

## 84 カードリーダー・ライタ

【図1】  
Logical Explanation of Invention  
発明の原理説明図

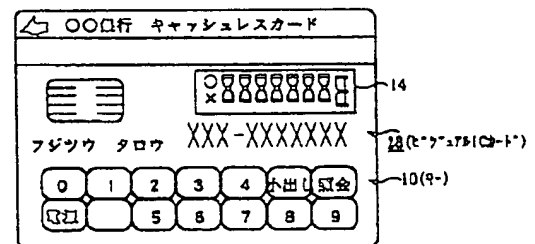
The diagram illustrates a data processing system with the following components and connections:

- Data Input Means:** Labeled "data input means" in handwritten text. It includes a sequence of input boxes labeled 10-1, 10-2, ..., 10-N, which feed into a "データ入力手段" (Data Input Means) block labeled 12.
- Display:** Labeled "Display" in handwritten text. It includes a "表示部" (Display Unit) labeled 14, which is connected to an "入力データ表示手段" (Input Data Display Means) block labeled 16. The entire display section is labeled "display means" in handwritten text.
- Application Processing:** The "データ入力手段" (12) feeds into an "アプリケーション処理手段" (Application Processing Means) block labeled 18.
- Discrimination:** The "アプリケーション処理手段" (18) feeds into a "判別データ処理手段" (Discrimination Data Processing Means) block labeled 20.
- Data Comparison:** The "判別データ処理手段" (20) feeds into a "データ照合手段" (Data Comparison Means) block labeled 22.
- Output:** The "データ照合手段" (22) feeds into an "表示データ出力手段" (Display Data Output Means) block labeled 24, which then feeds into a "本人照出手段" (Person Identification Means) block labeled 26.
- Feedback Loop:** A dashed line connects the "表示データ出力手段" (24) back to the "アプリケーション処理手段" (18).

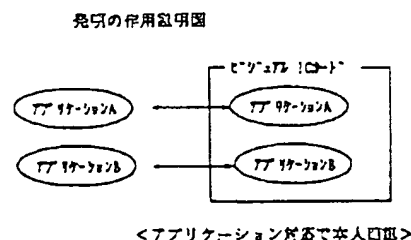
Handwritten annotations include:

- "discrimination data processing means" near block 20.
- "data comparison means" near block 22.
- "person identification means" near block 26.
- "application processing means" near block 18.
- "input data display means" near block 16.
- "data input means" near block 12.
- "display means" near block 14.

## ビジュアルICカードの外口説明

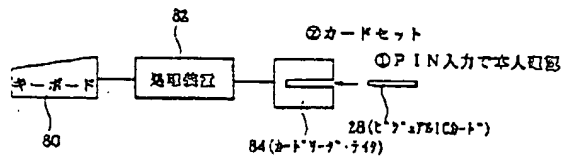


【图 3】



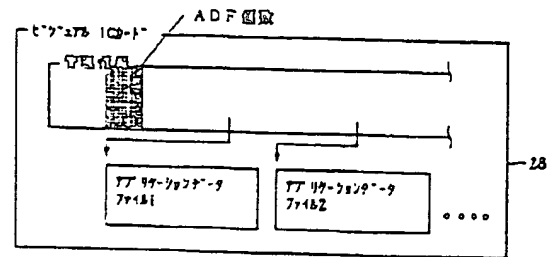
【図4】

実例のカードを取り扱うシステムの構成説明図



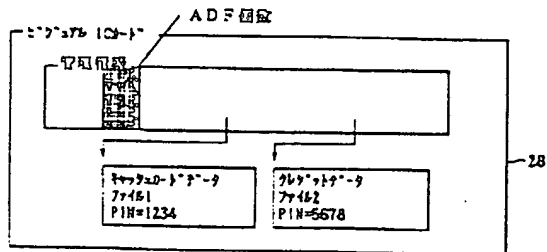
【図5】

実例のファイル構成説明図



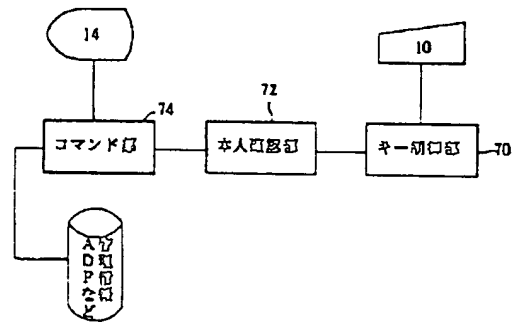
【図6】 file structure

実例の具体的なファイル構成説明図



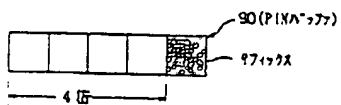
【図7】

実例の内部構成説明図



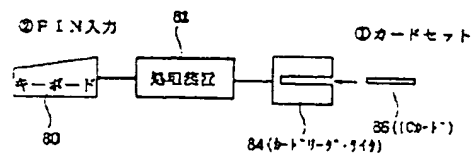
【図10】

実例で用いられるPINバッファの構成説明図



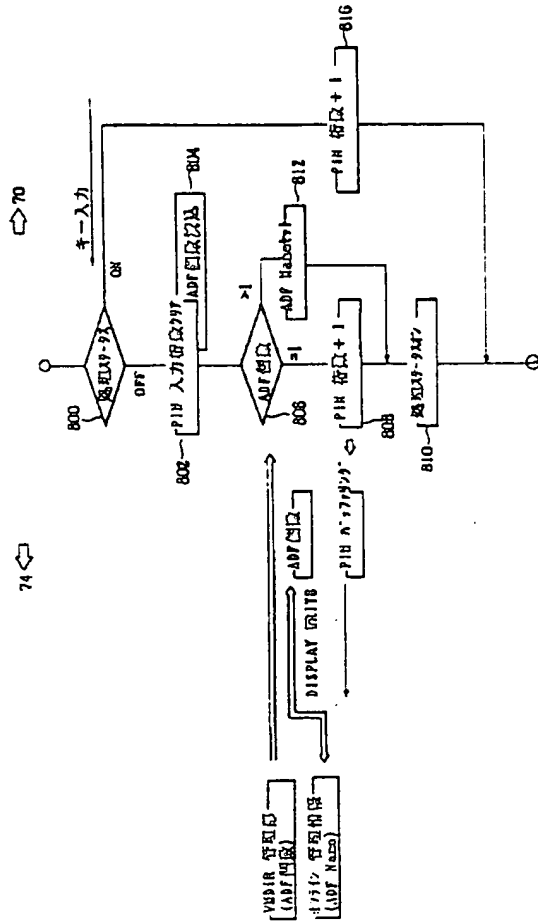
【図11】

ICカードシステムの構成説明図



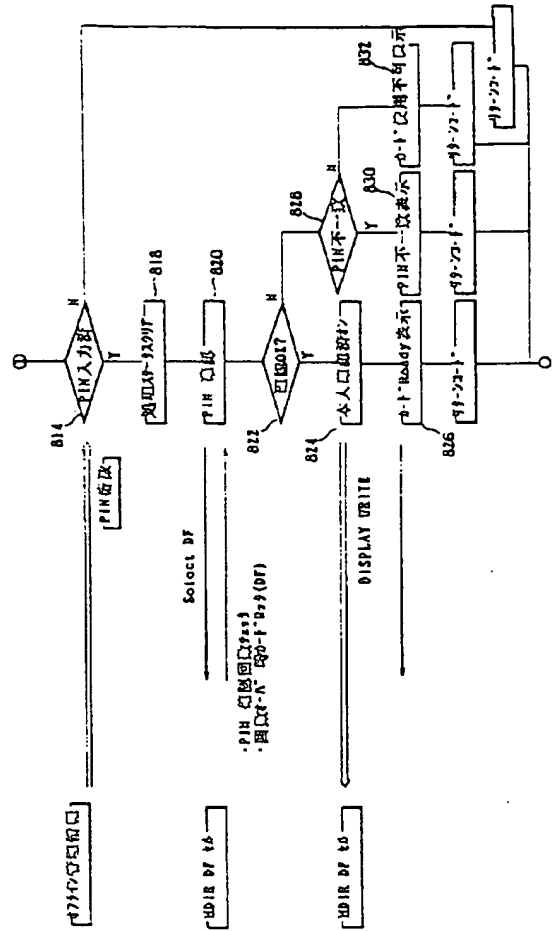
【圖 8】

### 突如閃の作用を説明するフローチャート



【図 9】

### 実地研の作用を説明するフローチャート

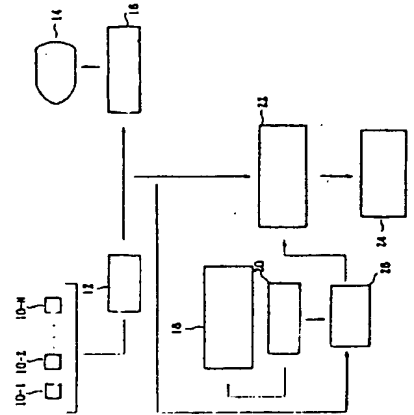


# (54) VISUAL IC CARD

(11) 4-255089 (A) (43) 10.9.1992 (19) JP  
 (21) Appl. No. 3-36674 (22) 6.2.1991  
 (71) FUJITSU LTD (72) HIROSHI TANAKA  
 (51) Int. Cl<sup>5</sup>. G06K19/10, B42D15/10, G06K19/07

**PURPOSE:** To provide an extremely effective visual IC card having many functions and excellent security with respect to an ID card to be used for a cash card, a credit card, a medical card, etc., especially provided with an input key and a display device.

**CONSTITUTION:** A data input means 12 inputs data corresponding to the operation of keys 10-1 to 10-N and an input data display means 16 displays the inputted data on a display device 14. Plural applications are previously written in an application storing means 18 and an identification(ID) data storing means 20 previously stores application ID data. A data collating means 22 collates the inputted data with the application ID data and a person-confirming means 24 confirms ~~x~~ card user as *the* ~~its~~ *the* owner when a positive collated result is obtained.



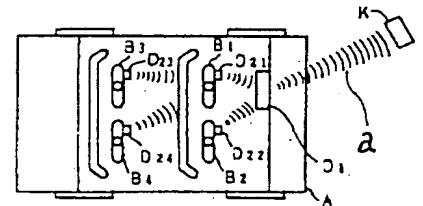
26: ID data reading means

# (54) IDENTIFICATION SYSTEM FOR VEHICLE IN/OUT MANAGEMENT

(11) 4-255090 (A) (43) 10.9.1992 (19) JP  
 (21) Appl. No. 3-9585 (22) 30.1.1991  
 (71) MEIDENSHA CORP (72) KAZUYUKI KUMAKI  
 (51) Int. Cl<sup>5</sup>. G07C9/00, B42D15/10, G06F15/21, G06K17/00, G08G1/017

**PURPOSE:** To automatically execute vehicle identification(ID) and the personal ID of a person getting on a vehicle and to simplify management by making a vehicle ID device loaded on a vehicle to inquire a personal ID card carried by a person getting on the vehicle at the time of passing a gate and transmit a personal ID code together with a vehicle ID code to a vehicle detector.

**CONSTITUTION:** When a vehicle A passes a gate, the vehicle detector K sends an access signal to a vehicle ID device D<sub>1</sub>. The device D<sub>1</sub> transmits an inquiry signal from a transmission part to the inside of the vehicle at the period of about one minute. Persons B<sub>1</sub> to B<sub>4</sub> getting on the vehicle respectively carry respective personal ID cards D<sub>21</sub> or the like. After receiving the inquiry signal, respective cards D<sub>21</sub> or the like transmit personal ID codes. Each personal ID card is provided with an inherent queue time based on a registered number to prevent the generation of signal collision. The device D<sub>1</sub> transmits the vehicle ID code and the personal ID codes to the detector K. The detector K manages the IN/OUT of the vehicle and the persons getting on the vehicle in accordance with these codes.



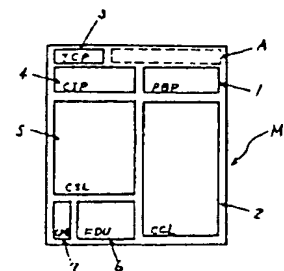
a: signal wave

# (54) CASH DISPENSER

(11) 4-255091 (A) (43) 10.9.1992 (19) JP  
 (21) Appl. No. 3-36901 (22) 6.2.1991  
 (71) NEC CORP (72) YOSHIMI KITAGAWA  
 (51) Int. Cl<sup>5</sup>. G07D1/00, G07D9/00

**PURPOSE:** To improve the operation convenience of a cash dispenser by providing the cash dispenser body with a consumption medium stock rack for storing consumption medium so as to always store the consumption medium.

**CONSTITUTION:** The cash dispenser body M is provided with a bankbook printer unit 1, a paper money processing unit 2, a card processing unit 4, or the like. The consumption medium stock rack A is arranged on a space position in the upper area of the dispenser body M. The stock rack A is formed by reinforced glass or reinforced plastic so that the inside can be observed and the number of remaining medium can be checked at a glance from the external. The stock rack A is laterally arranged and provided with a bankbook storing rack, a certificate storing rack, a receipt form storing rack, a journal form storing rack, a depositing/paying form storing rack, and a transfer card storing rack. Respective racks are provided with locking keys so as to store important medium.





特開平4-255089

(43) 公開日 平成4年(1992)9月10日

(51) Int.Cl.<sup>5</sup>

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 K 19/10

B 4 2 D 15/10

G 0 6 K 19/07

5 2 1

9111-2C

8623-5L

8623-5L

G 0 6 K 19/ 00

R

J

審査請求 未請求 請求項の数3(全6頁)

(21) 出願番号

特願平3-36674

(22) 出願日

平成3年(1991)2月6日

Application  
Date

Feb. 6, 1991

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72) 発明者 田中 弘

神奈川県川崎市中原区上小田中1015 富士

通株式会社内

(74) 代理人 弁理士 伊藤 儀一郎

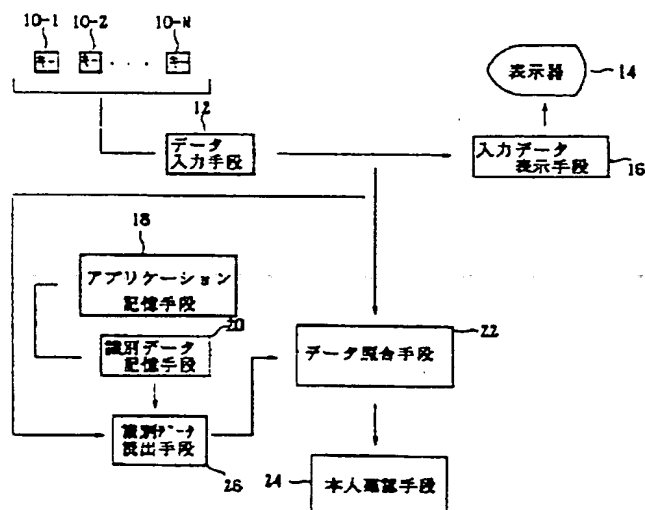
(54) 【発明の名称】 ビジュアル I C カード

(57) 【要約】

【目的】 本発明は、キャッシュカード、クレジットカード、医療カードなどに利用される I C カードにかかり、特に、入力キーと表示器が設けられた I C カードに関し、多機能でセキュリティに優れた極めて有用なビジュアル I C カードの提供を目的とする。

【構成】 キー 10-1、10-2・・・10-N の操作に応じたデータをデータ入力手段 12 が入力し、入力データ表示手段 16 は入力されたデータを表示器 14 に表示させる。アプリケーション記憶手段 18 には複数のアプリケーションが予め書き込まれ、識別データ記憶手段 20 はアプリケーション識別用のデータを予め記憶する。データ照合手段 22 は入力されたデータをアプリケーションの識別データと照合し、本人確認手段 24 は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

発明の原理説明図



1

## 【特許請求の範囲】

【請求項1】 キー（10-1, 10-2・・・10-N）の操作に応じたデータを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたデータをアプリケーションの識別データと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアルICカード。

【請求項2】 キー（10-1, 10-2・・・10-N）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（26）と、入力されたアプリケーション固有データを読み出されたアプリケーション識別用のデータと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときにカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアルICカード。

【請求項3】 キー（10-1, 10-2・・・10-N）の操作に応じアプリケーション特定データとアプリケーション固有データを入力するデータ入力手段（12）と、入力されたデータを表示器（14）に表示させる入力データ表示手段（16）と、複数のアプリケーションが予め書き込まれたアプリケーション記憶手段（18）と、アプリケーション識別用のデータを予め記憶する識別データ記憶手段（20）と、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを読み出す識別データ読出手段（26）と、入力されたアプリケーション固有データを読み出されたアプリケーションの識別データと照合するデータ照合手段（22）と、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を行なう本人確認手段（24）と、を有する、ことを特徴としたビジュアルICカード。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、キャッシュカード、クレジットカード、医療カードなどとして利用されるICカードにかかり、特に、入力キーと表示器が設けられたICカードに関する。

2

【0002】 この種のICカードには入力キーと表示器が設けられており、したがって、それらを用いてカード利用者の本人確認をカード単体で行なうことが可能となる。

## 【0003】

【従来の技術】 図11にはICカードシステムが示されており、キーボード80が処理装置82（パーソナルコンピュータなど）に設けられている。

【0004】 この処理装置82にはカードリーダー・ライター84が接続されており、ICカード86はカードリーダー・ライター84にセットされる。

【0005】 そして、キーボード80の操作で処理装置82にPINデータが入力されると、この入力データがICカード86へ送信される。

【0006】 その結果、カード利用者の本人確認が行なわれると、ICカード86を利用した取引が行なわれる。

【0007】 ところがこのシステムにおいては、本人確認用のPINデータが処理装置82へ入力されるので、PINデータの漏洩を確実に防止することが困難となる。

【0008】 そこで、図2のように複数のキー10と表示器14とを備え、これらキー10、表示器14によってカード利用者の本人確認をカード単体で行なえるビジュアルICカード28が利用される。

【0009】 従来においては、ビジュアルICカード28に単一のアプリケーションが用意されており、したがって、その用途はキャッシュカード、クレジットカード、医療カードなどのいずれかに限られていた。

## 【0010】

【発明が解決しようとする課題】 MSカード（磁気カード）にはキャッシュカード、クレジットカードの機能が既に付与されているので、これより能力がはるかに高いビジュアルICカード（28）にはより豊富な機能が要望される。

【0011】 本発明は上記従来の事情に鑑みてなされたものであり、その目的は、PINデータの漏洩を確実に防止できる多機能なビジュアルICカードを提供することにある。

## 【0012】

【課題を解決するための手段】 上記目的を達成するために、本発明にかかるビジュアルICカード（28）は図1のように構成されている。

【0013】 第1発明においては、キー10-1, 10-2・・・10-Nの操作に応じたデータをデータ入力手段12が入力し、入力データ表示手段16は入力されたデータを表示器14に表示させる。

【0014】 また、アプリケーション記憶手段18には複数のアプリケーションが予め書き込まれ、識別データ記憶手段20はアプリケーション識別用のデータを予め

記憶する。

【0015】そして、データ照合手段22は入力されたデータをアプリケーションの識別データと照合し、本人確認手段24は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【0016】第2の発明においては、キー10-1、10-2・・・10-Nの操作に応じアプリケーション特定データとアプリケーション固有データをデータ入力手段12が入力し、入力されたアプリケーション特定データと対応したアプリケーション識別用のデータを識別データ読出手段26が読み出す。

【0017】データ照合手段22は入力されたアプリケーション固有データを読み出された各アプリケーションの識別データと照合し、本人確認手段24は肯定的な照合結果が得られたときにカード利用者の本人確認を行なう。

【0018】第3に発明においては、肯定的な照合結果が得られたときに該当のアプリケーションについてのみカード利用者の本人確認を本人確認手段24が行なう。

【0019】

【作用】第1発明では、キー操作入力のデータをアプリケーションの識別データと照合した結果が肯定的なときに、カード利用者の本人確認が行なわれるので、カード利用者が本人であることと目的の機能（アプリケーション）を確認することが可能となる。

【0020】第2の発明では、目的の機能がカード利用者により特定されてから、そのアプリケーションに関する識別データとキー操作入力のデータが照合される。

【0021】第3の発明では、第2発明において肯定的な照合結果が得られた機能についてのみ、カード利用者の本人確認が行なわれる（図3参照）。

【0022】

【実施例】以下、図面に基づいて本発明にかかるビジュアルICカードの好適な実施例を説明する。

【0023】図2において、ビジュアルICカード28には複数のキー10と表示器14が設けられており、これらを用いてカード利用者の本人確認がカード単体で行なわれる。

【0024】このビジュアルICカード28はその本人確認が行なわれてから図4のカードリーダー・ライター84にセットされ、したがって、PINデータをキーボード80から処理装置82へ入力することを省略してその漏洩を防止できる。

【0025】本実施例のビジュアルICカード28には図5のように複数のアプリケーションデータファイル(ADF)1、2・・・が格納されており、このカード28がキャッシュカード及びクレジットカードとして利用される場合には、図6のようにそれらのアプリケーションデータファイル(1、2)が格納される。

【0026】そして、カード管理情報にはアプリケーシ

ョンデータファイル1、2・・・の個数が含まれており、これらアプリケーションデータファイル1、2・・・には相異なるPINデータ（通常は4桁）が各々含まれる（図6では"1234"、"5678"）。

【0027】また、ビジュアルICカード28には図7のキー制御部70、本人確認部72、コマンド部74が設けられており、キー操作で得られたデータはキー制御部10から本人確認部72へ入力される。

【0028】さらに、カード管理情報やアプリケーションデータファイル1、2・・・はコマンド部74によりアクセスされ、このコマンド部74で表示部14が制御される。

【0029】図8、図9には本人確認部72で行なわれる処理の内容がフローチャートで示されており、キー入力を確認されると、処理ステータスのフラグがオンされているか否かが判断される（ステップ800）。

【0030】このフラグは電源の投入時にオフされており（電源の投入は図2の電源キーを操作することで行なわれる）、そのフラグ状態が確認されたときには、図10のように5桁長とされたPINバッファ90がクリアされる（ステップ802）。

【0031】さらに、アプリケーションデータファイル1、2・・・の数が読み出され（ステップ804）、その数が"1"かこれを越えているかが判定される（ステップ806）。

【0032】そして、アプリケーションデータファイルの数が"1"である場合（単機能カードの場合）には、入力データがPINバッファ90に格納されてその現行桁がインクリメントされ（ステップ808）、上記のフラグがオンされる（ステップ810）。

【0033】また、アプリケーションデータファイルの数が"1"を越えている場合（多機能カードの場合）には、キー入力データ（1桁）で示されるファイル名（そのファイルのPINデータ）が読み出され、セットされる（ステップ812）。

【0034】この後においては、4桁のキーデータがPINデータとして入力されるまで（ステップ814）、入力データをPINバッファ90に格納してその現行桁をインクリメントする処理（ステップ816）が繰り返される。

【0035】そして4桁のキーデータが（PINデータとして）入力されると（ステップ814）、処理ステータスのフラグがオフされる（ステップ818）。

【0036】次に、セット済みのファイル名（そのファイルに含まれたPINデータ）とキー操作入力のPINデータ（先頭4桁、最初に入力された後尾1桁はサフィックスとなる）とが突き合わされ（ステップ820・・・アプリケーションデータのファイル数が"1"である場合には、そのファイル名となるPINデータ）、両データの一致が確認されると（ステップ82

5

2)、確認フラグがオンされ(ステップ824)、“Ready”の表示が表示器14で行なわれる(ステップ826)。

【0037】これに対し、両データの不一致が確認された場合にはその旨が表示器14で表示され(ステップ828、830)、両データ不一致の確認が規定の回数だけ繰り返されると、“カード使用不可”の表示が表示器14で行なわれる(ステップ832)。

【0038】以上のように、最初のキー入力データでアプリケーション数が把握されて対応のデータファイル(1、2・・・のいずれか)が特定され、後続4桁のキー入力データと特定されたデータファイルのPINデータとが一致したときに、そのアプリケーション(カード機能)についてのみ、本人確認が行なわれる。

【0039】図6において、“2”に続き“5678”のキーデータがPINデータとして入力されると、アプリケーションデータファイル2のクレジットカード機能について、本人確認が行なわれる。

【0040】したがって本実施例によれば、PINデータの漏洩を確実に防止できる多機能なビジュアルICカード28を提供することが可能となる。

【0041】

【発明の効果】以上説明したように本発明によれば、多機能でセキュリティに優れた極めて有用なビジュアルICカードを提供できる。

【図面の簡単な説明】

6

【図1】発明の原理説明図である。

【図2】ビジュアルICカードの外観説明図である。

【図3】発明の作用説明図である。

【図4】実施例のカードを取り扱うシステムの構成説明図である。

【図5】実施例のファイル構造説明図である。

【図6】実施例の具体的なファイル構造説明図である。

【図7】実施例の内部構成説明図である。

【図8】実施例の作用を説明するフローチャート(その1)である。

【図9】実施例の作用を説明するフローチャート(その2)である。

【図10】実施例で用意されるPINバッファの構成説明図である。

【図11】ICカードシステムの構成説明図である。

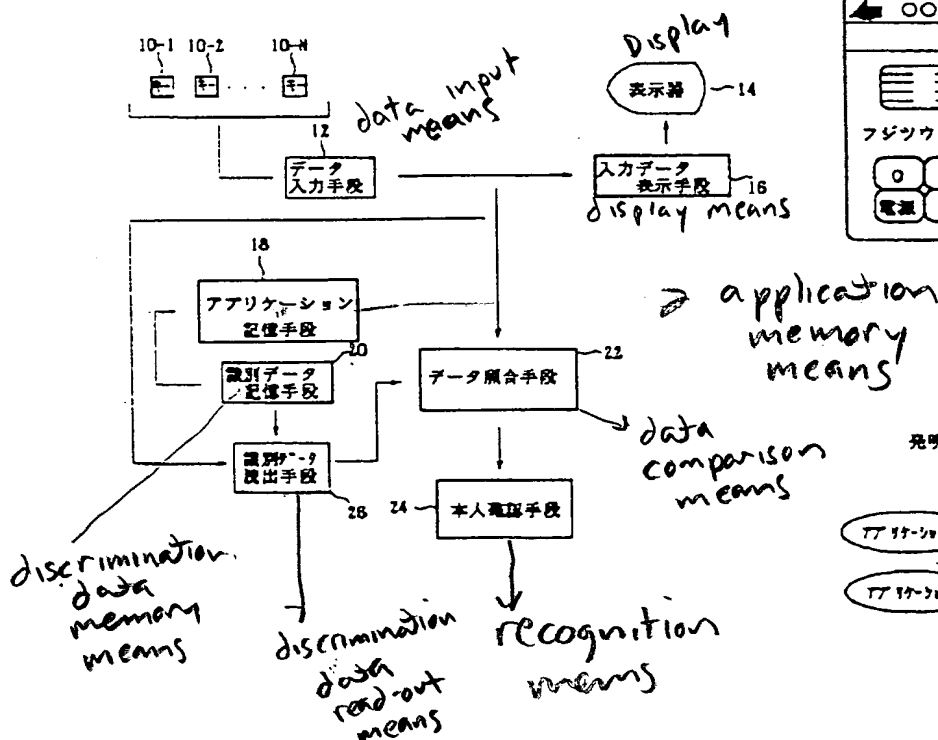
【符号の説明】

- 10 キー
- 14 表示部
- 28 ビジュアルICカード
- 70 キー制御部
- 72 本人確認部
- 74 コマンド部
- 80 キーボード
- 82 処理装置
- 84 カードリーダー・ライター

【図1】

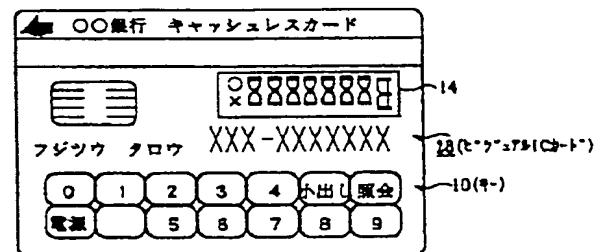
# Logical Explanation of Invention

発明の原理説明図



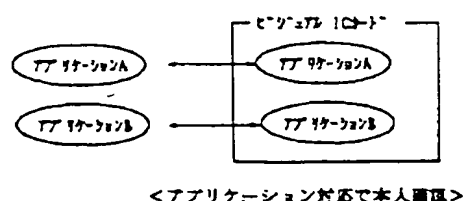
【図2】

ビジュアルICカードの外観説明図



【図3】

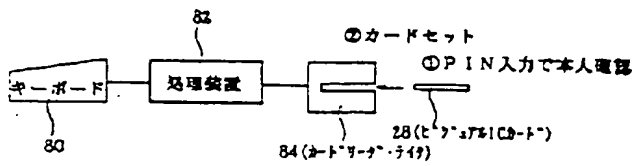
発明の作用説明図



<アプリケーション対応で本人確認>

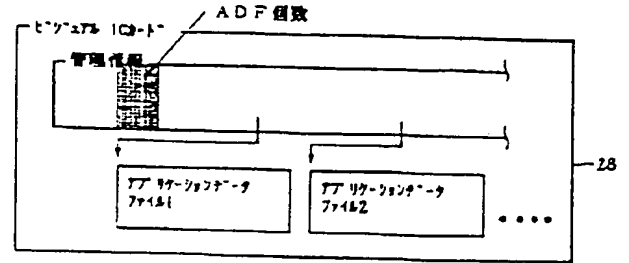
【図4】

実施例のカードを取り扱うシステムの構成説明図



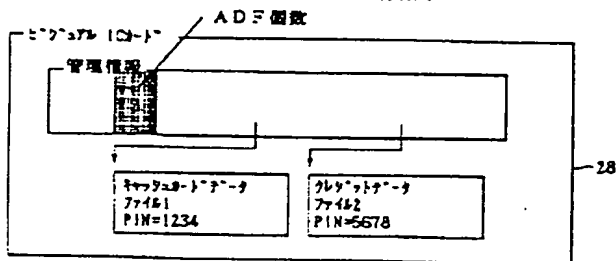
【図5】

実施例のファイル構成説明図



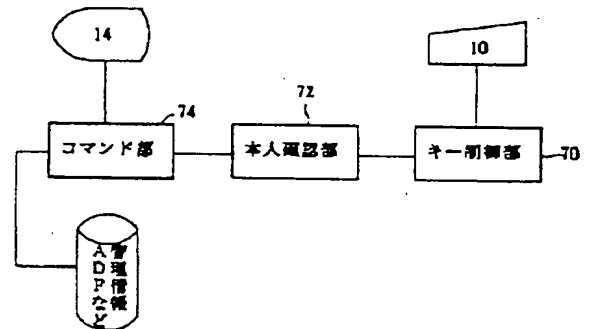
【図6】 file structure

実施例の具体的なファイル構成説明図



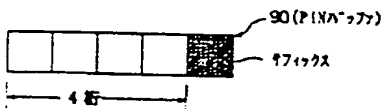
【図7】

実施例の内部構成説明図



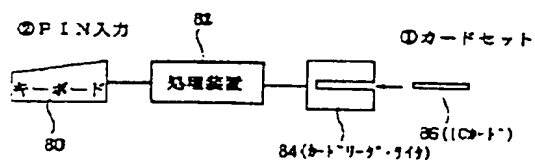
【図10】

実施例で用いられるPINバッファの構成説明図



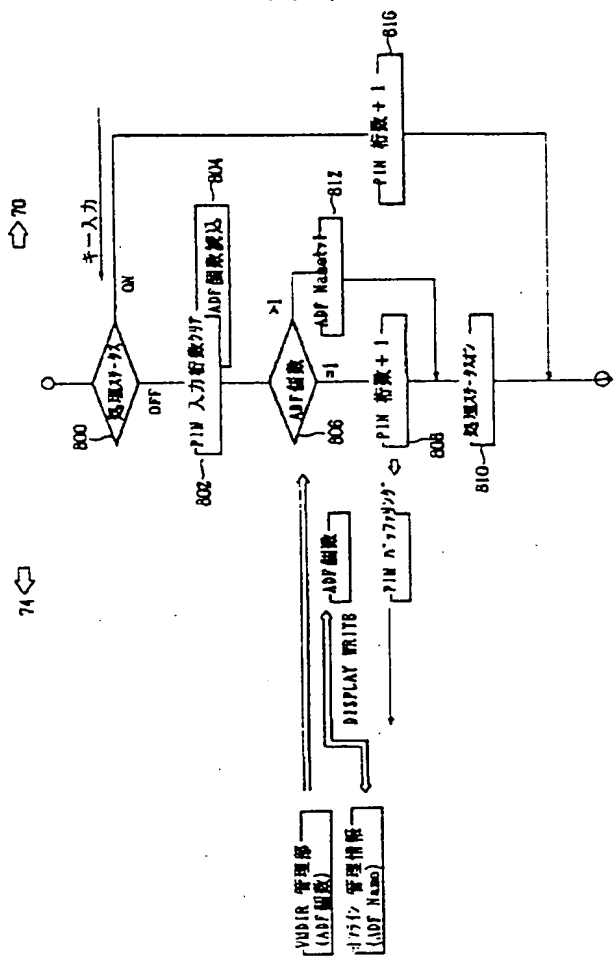
【図11】

ICカードシステムの構成説明図



【図8】

実施例の作用を説明するフローチャート



【図9】

実施例の作用を説明するフローチャート

